PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-216773
(43)Date of publication of application : 04.08.2000

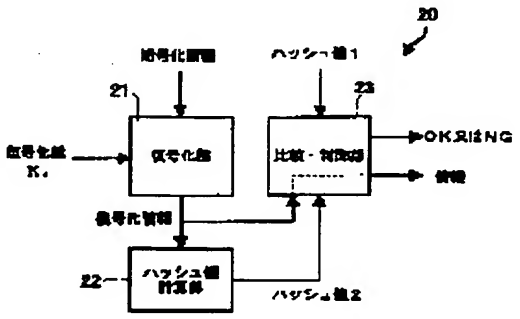
(51)Int.CI. H04L 9/32
G09C 1/00

(21)Application number : 11-014022
(22)Date of filing : 22.01.1999

(71)Applicant : TOYO COMMUN EQUIP CO LTD
(72)Inventor : SUGIMOTO KOICHI

(54) METHOD AND SYSTEM FOR DISCRIMINATING PROPRIETY OF ENCRYPTED INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a system for discriminating the propriety of encrypted information where a receiver side of the encrypted information can discriminate as to whether or not decoded information is correct.
SOLUTION: This system for discriminating propriety of encrypted information is provided with a means, that calculates a 1st hash value of the encrypted information on an information transmitter side by using a prescribed hash value generating algorithm, a means that transmits the 1st has value with the encrypted information, a means 22 that calculates a 2nd hash value of decoded information on an information receiver side by using the same algorithm as the hash value generating algorithm which calculates the 1st hash value, a means 23 that compares the received 1st hash value with the 2nd hash value, and a means 23 that discriminates that the decoded information is legitimate, when the 1st hash value coincides with the 2nd hash value.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－216773
（P2000－216773A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.'		識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ　9/00	６７５Ａ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	

審査請求　未請求　請求項の数２　ＯＬ　（全４頁）

(21)出願番号　特願平11－14022

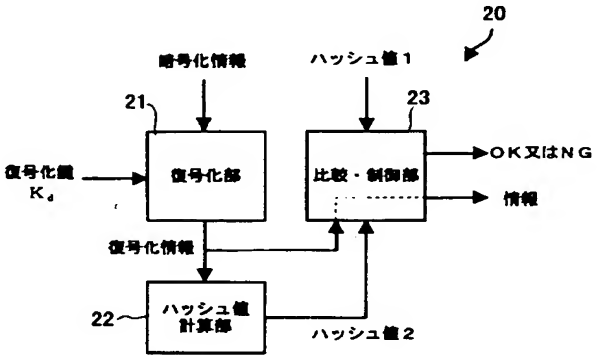
(22)出願日　平成11年１月22日(1999.1.22)

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　杉本　浩一
神奈川県高座郡寒川町小谷２丁目１番１号
東洋通信機株式会社内
(74)代理人　100098039
弁理士　遠藤　恭

Ｆターム(参考)　5J104 AA08 LA02 NA12 PA09

(54)【発明の名称】　暗号化情報の正当性を判断する方法及び装置

(57)【要約】
【課題】　暗号化された情報の受信側で、復号化した情報が正しいものであるか否かを判定することができる暗号化情報の正当性を判断する方法及び装置を提供する。
【解決手段】　本発明は、暗号化情報の正当性を判断する装置であって、情報の発信側で、所定のハッシュ値生成アルゴリズムにより、暗号化する情報の第１のハッシュ値を算出する手段１２と、上記第１のハッシュ値を、暗号化された上記情報と共に送信する手段と、上記情報の受信側で、復号化された上記情報の第２のハッシュ値を、上記第１のハッシュ値を算出したハッシュ値生成アルゴリズムと同じアルゴリズムにより算出する手段２２と、上記受信した第１のハッシュ値と上記第２のハッシュ値とを比較する手段２３と、上記第１のハッシュ値と上記第２のハッシュ値とが一致する場合に、上記復号化した情報が正当であると判断する手段２３とを備えて構成される。



1

【特許請求の範囲】
【請求項１】　暗号化情報の正当性を判断する方法であって、
情報の発信側で、所定のハッシュ値生成アルゴリズムにより、暗号化する情報の第１のハッシュ値を算出する手順と、
上記第１のハッシュ値を、暗号化された上記情報と共に送信する手順と、
上記情報の受信側で、復号化された上記情報の第２のハッシュ値を、上記第１のハッシュ値を算出したハッシュ値生成アルゴリズムと同じアルゴリズムにより算出する手順と、
上記受信した第１のハッシュ値と上記第２のハッシュ値とを比較する手順と、
上記第１のハッシュ値と上記第２のハッシュ値とが一致する場合に、上記復号化した情報が正当であると判断する手順と、を備えたことを特徴とする暗号化情報の正当性を判断する方法。
【請求項２】　暗号化情報の正当性を判断する装置であって、
情報の発信側で、所定のハッシュ値生成アルゴリズムにより、暗号化する情報の第１のハッシュ値を算出する手段と、
上記第１のハッシュ値を、暗号化された上記情報と共に送信する手段と、
上記情報の受信側で、復号化された上記情報の第２のハッシュ値を、上記第１のハッシュ値を算出したハッシュ値生成アルゴリズムと同じアルゴリズムにより算出する手段と、
上記受信した第１のハッシュ値と上記第２のハッシュ値とを比較する手段と、
上記第１のハッシュ値と上記第２のハッシュ値とが一致する場合に、上記復号化した情報が正当であると判断する手段と、を備えたことを特徴とする暗号化情報の正当性を判断する装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報を秘匿するための暗号化技術に関し、特に、暗号の受信側で、復号化された情報が正当なものであるか否かを判断するための方法及び装置に関する。
【０００２】
【従来の技術】従来より、電話機、無線通信装置及び情報通信装置等の通信システムにおいては、その通信システムの両端の通信当事者以外の者が、伝送される情報の内容を知ることができないようにするために、情報を暗号化して伝送することが行われている。
【０００３】情報を暗号化する場合、所定の暗号化アルゴリズムとこれに対応した所定の暗号化鍵が用いられ、同様に、暗号化された情報を復号化する場合には、所定

2

の復号化アルゴリズムとこれに対応した所定の復号化鍵が用いられる。一般に、暗号化アルゴリズム及び復号化アルゴリズムは公開され、復号化鍵は秘密にされる。一方で、暗号化鍵は公開される場合と、秘密にされる場合があり、暗号化鍵を公開する暗号系は公開鍵暗号系と呼ばれる。また、暗号化鍵と復号化鍵が同じ場合は、暗号化鍵を一般に公開することはできず、秘匿通信を行う相手にのみ知らせるようにする。このように、暗号化鍵と復号化鍵が等しい場合の暗号系は、対称鍵暗号系または共通鍵暗号系あるいは、秘密鍵暗号系と呼ばれる。
【０００４】暗号化された情報を正常に復号するためには、適切な復号化鍵（公開鍵暗号系の場合は、暗号化鍵と対応するものであり、共通鍵暗号系の場合は、暗号化鍵と同一のもの）を用いなければならない。適切な復号化鍵を用いない場合、受信側は元の情報を得ることができない。また、暗号化された情報が伝送される際に、伝送誤りが生じた場合も、受信側が復号したものは元の正しい情報に復号されない。
【０００５】
【発明が解決しようとする課題】暗号技術を利用した通信システムにおいて、暗号化された情報が正常に復号されない場合、正常に復号化されなかった情報を用いるとシステムに悪影響を及ぼすことがある。例えば、WWW (World Wide Web)ブラウザ上のコンテンツを暗号化する場合、情報が正常に復号されないと、無意味な情報がブラウザ上に表示されたり、ブラウザが異常終了したりすることがある。また、復号化した情報を用いて機器を制御する場合において、情報が正常に復号されないと、制御機器の正しい制御が行われないことがある。
【０００６】上述した事態を回避するためには、受信した暗号化情報が正しいものであるか否かを判定し、正常に復号できた場合にのみこれを用いるようにすれば良い。
【０００７】従って、本発明の目的は、情報の受信側で、復号化した情報が正しいものであるか否かを判定することにより、上記不具合を解消することができる暗号化情報の正当性を判断する方法及び装置を提供することにある。
【０００８】
【課題を解決するための手段】上記目的を達成するため本発明は、暗号化情報の正当性を判断する方法であって、情報の発信側で、所定のハッシュ値生成アルゴリズムにより、暗号化する情報の第１のハッシュ値を算出する手順と、上記第１のハッシュ値を、暗号化された上記情報と共に送信する手順と、上記情報の受信側で、復号化された上記情報の第２のハッシュ値を、上記第１のハッシュ値を算出したハッシュ値生成アルゴリズムと同じアルゴリズムにより算出する手順と、上記受信した第１のハッシュ値と上記第２のハッシュ値とを比較する手順と、上記第１のハッシュ値と上記第２のハッシュ値とが

一致する場合に、上記復号化した情報が正当であると判断する手順とを備えて構成される。

【０００９】また、本発明は、暗号化情報の正当性を判断する装置であって、情報の発信側で、所定のハッシュ値生成アルゴリズムにより、暗号化する情報の第１のハッシュ値を算出する手段と、上記第１のハッシュ値を、暗号化された上記情報と共に送信する手段と、上記情報の受信側で、復号化された上記情報の第２のハッシュ値を、上記第１のハッシュ値を算出したハッシュ値生成アルゴリズムと同じアルゴリズムにより算出する手段と、上記受信した第１のハッシュ値と上記第２のハッシュ値とを比較する手段と、上記第１のハッシュ値と上記第２のハッシュ値とが一致する場合に、上記復号化した情報が正当であると判断する手段とを備えて構成される。

【００１０】ここで、ハッシュ値とは、任意の長さの情報の特徴を抽出した値で、その情報と１対１の関係をもつ固定長のメッセージダイジェストをいう。ハッシュ値を算出するアルゴリズム(以下、ハッシュ値算出アルゴリズムという)としては、SHA(Secure Hash Algorithm)、RIPE-MD(Race Integrity Primitive Evaluation Message Digest)、MD5(Message Digest #5)等が知られており、本発明では、これら周知のアルゴリズムを用いてハッシュ値を算出することができる。また、一般のDES(Date Encryption Standard)などのブロック暗号技術を用いてハッシュ値を算出しても良い。

【００１１】一般に、ハッシュ値算出アルゴリズムは次のような性質を有する。

①ハッシュ値算出アルゴリズムを用いて算出したハッシュ値から、元の情報の一部を復元することは困難である。

②同一情報を同じハッシュ値算出アルゴリズムを用いてハッシュ値を算出すると、得られたハッシュ値は同じ値となる。

③異なる情報を同じハッシュ値算出アルゴリズムを用いてハッシュ値を算出すると、得られたハッシュ値は、高い確率で互いに異なる値となる。

【００１２】上記３つの性質から、ハッシュ値を暗号化情報の正当性を判断するために用いることは極めて有益である。上記①の性質により、ハッシュ値から元の情報が解読されるのが防止され、上記②及び③の性質により、暗号前と復号後の情報から算出されるハッシュ値を比較することにより、情報の正当性が保証される。すなわち、本発明において、第１のハッシュ値は暗号化前の情報から計算され、第２のハッシュ値は復号化した情報から算出される。従って、復号化された情報が正しいものでない場合、第１のハッシュ値と第２のハッシュ値は異なり、正しいものである場合、第１のハッシュ値と第２のハッシュ値は一致することになる。

【００１３】

【発明の実施の形態】以下、図示した一実施形態に基いて本発明を詳細に説明する。図１は、本発明に従って構成された暗号化装置のブロック図、図２は、同じく復号化装置のブロック図である。本発明に係る暗号化情報の正当性を判断する方法は、情報の送信側に備えられた図１の暗号化装置１０及び情報の受信側に備えられた図２の復号化装置２０によって達成される。

【００１４】図１に示すように、暗号化装置１０は、暗号化部１１及びハッシュ値計算部１２から構成される。暗号化部１１は、情報及び暗号化鍵Ｋｃを入力として、情報を暗号化し、結果を暗号化情報として出力する。ハッシュ値計算部１２は、情報を入力として、そのハッシュ値を計算し、結果をハッシュ値１として出力する。上記ハッシュ値１は、暗号化情報と共に、図示しない有線ネットワーク、無線通信手段、その他の送信手段によってその受信者へ送られる。

【００１５】図２に示すように、復号化装置２０は、復号化部２１、ハッシュ値計算部２２及び比較・制御部２３から構成される。復号化部２１は、上記暗号化装置１０から送信された暗号化情報と復号化鍵Ｋｄを入力として、暗号化情報を復号化し、結果を復号化情報として出力する。なお、上記復号化鍵Ｋｄは、この暗号・復号装置で用いられるアルゴリズムが公開鍵暗号系の場合には、暗号化鍵Ｋｃに対応するものが用いられ、共通鍵暗号系の場合には、暗号化鍵Ｋｃと同一のものが用いられる。

【００１６】ハッシュ値計算部２２は、復号化部２１の出力した復号化情報を入力として、そのハッシュ値を計算し、結果をハッシュ値２として出力する。ここで、ハッシュ値計算部２２は、図１におけるハッシュ値計算部１２と同じ構成のものが用いられる。すなわち、ハッシュ値計算部１２におけるハッシュ値計算アルゴリズムと同じアルゴリズムを、復号側のハッシュ値計算部２２に用いる。

【００１７】比較・制御部２３は、上記復号した情報が正しいもの、すなわち暗号前の情報と一致するか否かを判断し、一致すると判断された場合にのみ上記復号化された情報を有効な情報として出力するものである。比較・制御部２３は、暗号化装置１０から送信されたハッシュ値１、ハッシュ値計算部２２の出力したハッシュ値２、及び復号化部２１の出力した復号化情報を入力とする。入力されたハッシュ値１とハッシュ値２は、ここで比較され、両者が異なれば、復号化情報が正しくない、すなわち暗号前の情報が通信中あるいは復号化時に、何らかの事由により変化したと判断される。通信中のデータ改竄、通信ノイズによる情報ビットの変化、復号化鍵Ｋｄが暗号化鍵Ｋｃに対応していない場合等によって、上記ハッシュ値の相違が発生する。この場合、比較・制御部２３は、復号化情報が正しくないことを示すNG信号を出力する。受信側は上記NG信号を受けた場合、送信側に情報の再送信を求める等の対応を採ることができる。一

5

6

方、２つのハッシュ値１及び２が一致する場合は、復号化情報が正しいものであると判断して、OK信号を出力すると共に、上記復号化情報を出力する。

【００１８】以上、本発明の一実施形態を図面に沿って説明した。しかしながら本発明は前記実施形態に示した事項に限定されず、特許請求の範囲の記載に基いてその変更、改良等が可能であることは明らかである。上記暗号化装置及び復号化装置は、専用のハードウェアによって構成されるものであっても良いし、汎用のコンピュータ上で実行されるソフトウェアプログラムを含んで構成されるものであっても良い。

【００１９】

【発明の効果】以上の如く本発明によれば、ハッシュ値の性質を用いて、暗号化された情報の正当性を判断することができる。これによって、情報が正しくない場合に起こり得る装置の誤動作等の問題を最小にすることができる。

【図面の簡単な説明】

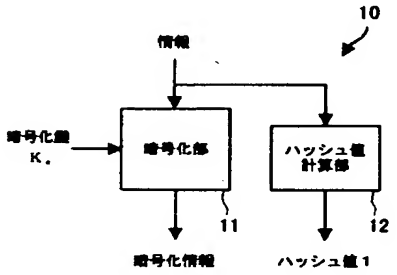
【図１】本発明に従って構成された暗号化装置のブロック図である。

【図２】本発明に従って構成された復号化装置のブロック図である。

【符号の説明】

１０　暗号化装置
１１　暗号化部
１２　ハッシュ値計算部
２０　復号化装置
２１　復号化部
２２　ハッシュ値計算部
２３　比較・制御部

【図１】



【図２】